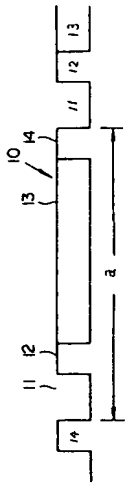
(54) DETECTION OF BIT SYNCHRONIZATION
(11) 61-260734 (A) (43) 18.11.1986 (19) JP
(21) Appl. No. 60-102462 (22) 14.5.1985
(71) KOMATSU LTD (72) YOSHIO ASAYAMA(2)
(51) **Int. Cl⁴. H04L7/06,H04L7/04**

PURPOSE: To prevent mis-recognition of data by setting a synchronous bit while a different bit width is given from other data and measuring the bit width so as to detect the bit thereby preventing the deviation of synchronization at error restoration.

CONSTITUTION: One frame of a data signal 10 consists of a synchronous bit (start bit) 11 of an L level set by 1.5-bit, a one-bit H level open bit 12, a data bit 13 comprising a pescribed bit number and a 1-bit H level stop bit 14. Thus, the bit number of the synchronous bt and the bit number of the data bit are distinguished, the synchronization deviation of error restoration is provented to prevent mis-recognition of data thereby reducing the restoration time and improving the transmission efficiency.

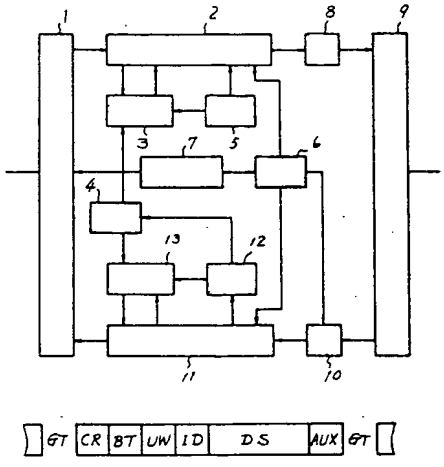


a: 1 frame

(54) TIME DIVISION MULTIPLEX ACCESS CIPHERING COMMUNICATION SYSTEM
(11) 61-260735 (A) (43) 18.11.1986 (19) JP
(21) Appl. No. 60-102017 (22) 14.5.1985
(71) FUJITSU LTD (72) AKIRA KAWASAKI(2)
(51) **Int. Cl⁴. H04L9/02,H04J3/00**

PURPOSE: To reduce the quantity of information relating to the ciphering key in use by allowing a sender station to use a change in a synchronous word so as to inform the kind of the ciphering key and the revision period to a reception station.

CONSTITUTION: A sending data DS is ciphered by a ciphering section 3, a prescribed word in synchronous words UW prepared by a synchronous word generating section 5, a data burst is combined and the result is sent via a modulation section 8 and a transmission/reception device 9. When the sending station revises the ciphering key in use at preset into the next ciphering key, the kind of the synchronous words UW is changed for a predetermined number of times and then sent. On the other hand, when a synchronous word detection section 12 of the reception station recognizes the change of the transmited synchronous word UW, it is informed to a cihpering key generating section 4 and a decoding section 13. When the number of times of changes reaches a predetermined number of times, a ciphering key generating section 4 revises the ciphering key in use so far into the next ciphering key and sends the result to a ciphering section 3 and a decoding section 13.

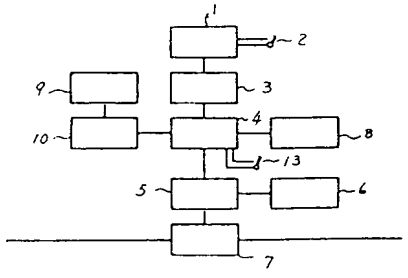


1: ground line connection interface, 2: burst combining section, 6: synchronous control section, 7: time slot assigning control section, 10: demodulation section, 11: burst decomposing section

(54) SYSTEM OF FORMING GROUP CIPHRING KEY
(11) 61-260736 (A) (43) 18.11.1986 (19) JP
(21) Appl. No. 60-102027 (22) 14.5.1985
(71) FUJITSU LTD (72) AKIRA KAWASAKI(2)
(51) **Int. Cl⁴. H04L9/02**

PURPOSE: To simplify the ciphering communication in a group by providing a group mode in addition to a normal mode and generating a common variable to the group when the group mode is set thereby forming a ciphering key in common to the group.

CONSTITUTION: A mode setting section 8 as a means setting the group mode in addition to the normal mode is provided and when the group mode is set, an identification number input section 9 and a collation section 10 are provided as a means generating a common variable to the group. Since a ciphering device set to the group mode generates a common variable, a common base key is formed with an optional ciphering device in the group, the forming and management of the ciphering key are simplified while the 2-layer management system is applied to facilitate the ciphering communication in the group.



1: power supply section, 3: power supply detection section, 4: key generating section, 5: ciphering key operating section, 6: key input section, 7: ciphering processing section, 8: mode setting section

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭61－260735

⑤Int.Cl.⁴	識別記号	庁内整理番号	㊸公開　昭和61年(1986)11月18日
H 04 L 9/02		Z－7240－5K	
H 04 J 3/00		C－8226－5K	

審査請求　未請求　発明の数 2　（全6頁）

㊹発明の名称　時分割マルチプルアクセス暗号通信方式

㉑特　願　昭60－102017

㉒出　願　昭60(1985)5月14日

㉒発明者　川崎　昱　川崎市中原区上小田中1015番地　富士通株式会社内

㉒発明者　妹尾　雅之　川崎市中原区上小田中1015番地　富士通株式会社内

㉒発明者　太田　幸一　川崎市中原区上小田中1015番地　富士通株式会社内

㉑出願人　富士通株式会社　川崎市中原区上小田中1015番地

㉔代理人　弁理士　松岡　宏四郎

明　細　書

1. 発明の名称

時分割マルチプルアクセス暗号通信方式

2. 特許請求の範囲

(1) 送信局がデータ送信用のバーストに同期語を付加して送出する時分割マルチプルアクセス通信システムにおいて、前記送信局が前記同期語に予め定められた変更を所定回数実行することにより、前記バーストにより伝送するデータの暗号化および復号化に使用する暗号鍵に所定の更新を行う時期を受信局に通知することを特徴とする時分割マルチプルアクセス暗号通信方式。

(2) 送信局がデータ送信用のバーストに同期語を付加して送出する時分割マルチプルアクセス通信システムにおいて、前記送信局が前記同期語に行う予め定められた変更の種類と、前記バーストに付加する暗号鍵を識別する情報との組合わせにより、該バーストにより伝送するデータの暗号化および復号化に使用する暗号鍵の種類を受信局に指定することを特徴とする時分割マルチプルアクセス暗号通信方式。

3. 発明の詳細な説明

〔概要〕

送信局がデータ送信用のバーストに同期語を付加して送出する時分割マルチプルアクセス（TDMA）通信システムにおいて、送信局が同期語の変化を用いて暗号鍵の種類、更新時期を受信局に通知することにより、使用暗号鍵に関する情報量を削減するものである。

〔産業上の利用分野〕

本発明は時分割マルチプルアクセス通信システムを経由して暗号通信を行う時分割マルチプルアクセス暗号通信方式に関する。

暗号通信においては、送信側で送信データを予め定められた規約（以後暗号鍵と称する）に基づき暗号化して送信し、受信側で送信側と同一の暗号鍵に基づき復号化する。暗号化および復号化の為に使用する暗号鍵を複数種類準備し、適宜変更して使用することが、暗号化データの秘匿強度を向上する為に有効である。かかる場合に、送信側

で使用している暗号鍵を受信側に認識させる必要がある。

この種の暗号通信を時分割マルチプルアクセス通信システムを経由して実行する場合には、送信側から受信側へ現在使用中の暗号鍵の種類を通知する情報量は、極力削減されることが望ましい。

〔従来の技術〕

第5図は時分割マルチプルアクセス衛星通信システムにおける従来ある時分割マルチプルアクセス暗号通信方式の一例を示す図であり、第6図は第5図におけるデータバーストの一例を示す図である。

送信局において、地上回線から地上回線接続インタフェース1を介してバースト組立部2に送信データDSが到着すると、バースト組立部2は、送信データDSを暗号化部3に伝達する。

暗号化部3は、暗号鍵発生部4が準備する複数種類（例えばk種類）の暗号鍵の中の、現在使用する暗号鍵に基づき送信データを暗号化し、バースト組立部2に返送する。

バースト組立部2は、暗号化部3から返送される暗号化された送信データDSに、送信局識別情報ID、暗号鍵発生部5から伝達される使用中の暗号鍵に関する識別情報（以後暗号鍵識別情報KEYと称する）、或いは同期語発生部5が作成するバースト同期確立用の同期語UW、更に受信局でデータバーストを受信するに必要な搬送波再生部CR、ビット再生部BT、並びに誤り検出符号その他の補助部AUXを付加して第2図に示す如きデータバーストを組立て、同期制御部6およびタイムスロット割当制御部7により指定される時間領域に、変調部8および送受信装置9を経由して衛星通信回線に送出する。なお第2図におけるGTは、隣接バーストとの衝突を防止するガード時間である。

一方受信局においては、復調部10が衛星通信回線から送受信装置9を経由して到着する信号の中から、同期制御部6およびタイムスロット割当制御部7により指定された時間領域に受信したデータバーストを搬送波再生部CRおよびビット再

生部BTを用いて復調し、バースト分解部11に伝達する。

バースト分解部11は、伝達されるデータバーストを分解し、同期語UWは同期語検出部12に伝達してバースト同期を確立させ、暗号化された送信データDSおよび暗号鍵識別情報KEYは復号化部13に伝達する。

復号化部13は、暗号鍵発生部4が準備する複数種類の暗号鍵の中から、受信した暗号鍵識別情報KEYに基づき、復号化に使用すべき暗号鍵を識別し、バースト組立部2から伝達された暗号化され送信データDSを識別した暗号鍵により復号化してバースト組立部2に返送する。

バースト組立部2は、復号化部13から返送された復号化された送信データDSを、地上回線接続インタフェース1を介して地上回線に送出する。

〔発明が解決しようとする問題点〕

以上の説明から明らかな如く、従来ある時分割マルチプルアクセス暗号通信方式においては、送信局は送信データDSを暗号化するに使用した暗

号鍵を、暗号鍵識別情報KEYのみにより識別してデータバーストに付加していた。従って暗号鍵識別情報KEYの情報量が増加し、データバーストの他の情報を圧迫する恐れがあった。

〔問題点を解決するための手段〕

本発明は下記の手段を講ずることにより、前記問題点を解決する。

即ち本第一の発明においては、送信局が同期語に予め定められた変更を所定回数実行することにより、バーストにより伝送するデータの暗号化および復号化に使用する暗号鍵に所定の更新を行う時期を受信局に通知する。

また本第二の発明においては、送信局が同期語に行う予め定められた変更の種類と、バーストに付加する暗号鍵を識別する情報との組合わせにより、バーストにより伝送するデータの暗号化および復号化に使用する暗号鍵の種類を受信局に指定する。

〔作用〕

即ち本第一の発明によれば、暗号鍵の更新時期

は同期語の変更により伝達される為、データバーストに付加すべき暗号鍵を識別する情報が不要となる。

また本第二の発明によれば、データバーストに付加すべき暗号鍵を識別する情報量の一部が同期語により伝達される為、暗号鍵を識別する情報の情報量が削減される。

〔実施例〕

以下、本発明の一実施例を図面により説明する。第1図は本第一の発明の一実施例による時分割マルチプルアクセス暗号通信方式を示す図であり、第2図は第1図におけるデータバーストの一例を示す図であり、第3図は本第二の発明の一実施例による時分割マルチプルアクセス暗号通信方式を示す図であり、第4図は第3図におけるデータバーストの一例を示す図でる。なお、全図を通じて同一符号は同一対象物を示す。

第1図においては、送信局が暗号化に使用する暗号鍵、および受信局が復号化に使用する鍵は、暗号鍵発生部4が予め準備するm種類の暗号鍵を、

予め定められた順序で交換して使用するものとし、送信局および受信局において当初使用する暗号鍵は、予め一致されているものとする。また同期語発生部5は複数種類（例えばm種類）の同期語ＵＷを準備している。

また第2図においては、暗号鍵識別情報ＫＥＹがデータバーストから除去されている。

送信局においては、バースト組立部2が、地上回線から地上回線接続インタフェース1を介して伝達される送信データＤＳを暗号化部3により暗号化し、同期語発生部5が準備する同期語ＵＷの中の所定の一個を選び、搬送波再生部ＣＲ、ビット再生部ＢＴ、送信局識別情報ＩＤ、並びに誤り検出符号その他の補助部ＡＵＸと共に、第4図に示す如きデータバーストを組立て、変調部8および送受信装置9を介して衛星通信回線に送信する。

送信局が現在使用中の暗号鍵を次の暗号鍵に更新する場合には、同期語ＵＷの種類を予め定められた回数（例えば1回）変更して送信する。

一方受信局においては、バースト分解部11が、

復調部10から伝達されるデータバーストを分解し、同期語ＵＷは同期語検出部12に伝達してバースト同期を確立させ、暗号化された送信データＤＳは復号化部13に伝達する。なお同期語検出部12は、検出した同期語ＵＷの種類を暗号鍵発生部4および復号化部13にも伝達する。

復号化部13は、当初予め定められた暗号鍵を用いて、バースト組立部2から伝達された暗号化され送信データＤＳを識別した暗号鍵により復号化してバースト組立部2に返送する。

なお同期語検出部12が伝達された同期語ＵＷが変更されたことを識別すると、その旨暗号鍵発生部4および復号化部13に通知する。暗号鍵発生部4は変更回数が予め定められた回数（例えば1回）に達すると、夫迄使用していた暗号鍵を次の暗号鍵に更新し、暗号化部3および復号化部13に伝達する。以後復号化部13は、新たに変更された暗号鍵を用いて、バースト分解部11から伝達される暗号化された送信データＤＳを復号化する。

従って送信局から衛星通信回線に送信されるデータバーストには、暗号鍵識別情報ＫＥＹを付加する必要が無くなる。

次に第3図においても、同期語発生部5は複数種類（例えばm種類）の同期語ＵＷを準備している。

送信局においては、バースト組立部2が、地上回線から地上回線接続インタフェース1に到着する送信データＤＳを暗号化部3により暗号化し、同期語発生部5が準備する同期語ＵＷの中の所定の一個を選び、暗号鍵発生部4から伝達される暗号鍵識別情報ＫＥＹ、搬送波再生部ＣＲ、ビット再生部ＢＴ、送信局識別情報ＩＤ、並びに誤り検出符号その他の補助部ＡＵＸと共に、第4図に示す如きデータバーストを組立てる。

なお暗号鍵の識別は、暗号鍵識別情報ＫＥＹおよび同期語ＵＷの組合わせで識別させる為、暗号鍵識別情報ＫＥＹの種類は、第5図および第6図の場合に比し1／mに減少する。従ってデータバーストに付加すべき暗号鍵識別情報ＫＥＹの所要

情報量（ビット数）も第２図に示す如く減少する。

一方受信局においては、バースト分解部１１が、復調部１０から伝達されるデータバーストを分解し、同期語ＵＷは同期語検出部１２に伝達してバースト同期を確立させ、暗号化された送信データＤＳおよび暗号鍵識別情報ＫＥＹを復号化部１３に伝達する。なお同期語検出部１２は、検出した同期語ＵＷを復号化部１３にも伝達する。

復号化部１３は、暗号鍵識別情報ＫＥＹと、同期語検出部１２から伝達される同期語ＵＷとの組合わせに基づき、暗号鍵発生部５が準備する複数種類（ｋ種類）の暗号鍵の中から、復号化に使用すべき暗号鍵を識別し、バースト組立部２から伝達された暗号化され送信データＤＳを識別した暗号鍵により復号化してバースト組立部２に返送する。

なお、第１図乃至第４図はあく迄本発明の一実施例に過ぎず、例えばデータバーストの構成は図示されるものに限定されることは無く、他に幾多の変形が考慮されるが、何れの場合にも本発明の効果は変わらない。また送信局および受信局の構成は図示されるものに限定されることは無く、他に幾多の変形が考慮されるが、何れの場合にも本発明の効果は変わらない。更に本発明の対象となる時分割マルチプルアクセス通信システムは、衛星通信システムに限定されぬことは言う迄も無い。

〔発明の効果〕

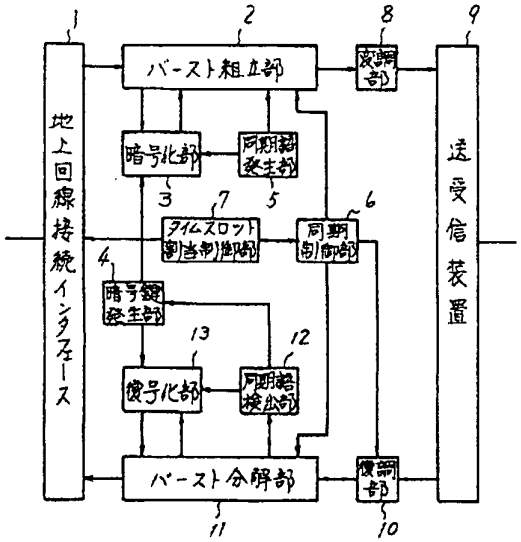
以上本発明によれば、前記時分割マルチプルアクセス通信システムにおいて、本第一の発明によれば、データバーストに付加すべき暗号鍵を識別する情報が不要となり、また本第二の発明によれば、データバーストに付加すべき暗号鍵を識別する情報量が削減され、データバースト内の他の情報量を圧迫する恐れが解消される。

4. 図面の簡単な説明

第１図は本第一の発明の一実施例による時分割マルチプルアクセス暗号通信方式を示す図、第２図は第１図におけるデータバーストの一例を示す図、第３図は本第二の発明の一実施例による時分割マルチプルアクセス暗号通信方式を示す図、第４図は第３図におけるデータバーストの一例を示す図、第５図は従来ある時分割マルチプルアクセス暗号通信方式の一例を示す図、第６図は第５図におけるデータバーストの一例を示す図である。

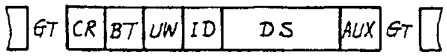
図において、１は地上回線接続インタフェース、２はバースト組立部、３は暗号化部、４は暗号鍵発生部、５は同期語発生部、６は同期制御部、７はタイムスロット割当制御部、８は変調部、９は送受信装置、１０は復調部、１１はバースト分解部、１２は同期語検出部、１３は復号化部、ＡＵＸは補助部、ＢＴはビット再生部、ＣＲは搬送波再生部、ＤＳは送信データ、ＧＴはガード時間、ＩＤは送信局識別情報、ＫＥＹは暗号鍵識別情報、ＵＷは同期語、を示す。

代理人　弁理士　松岡宏四郎



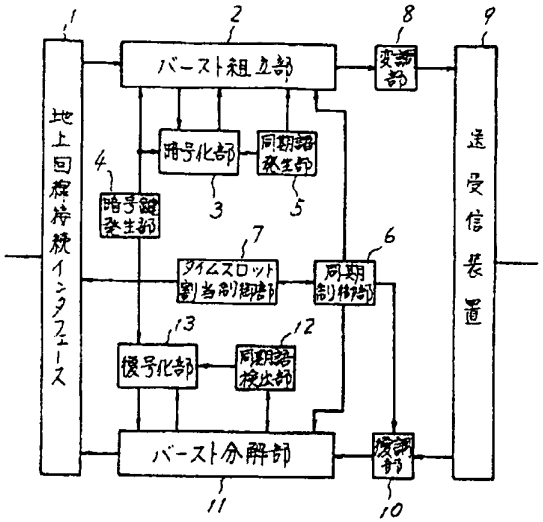
本第一の発明の実施例を示す図

第 1 図



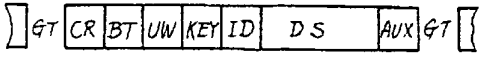
本第一の発明のデータバーストを例示する図

第 2 図



本第二の発明の実施例を示す図

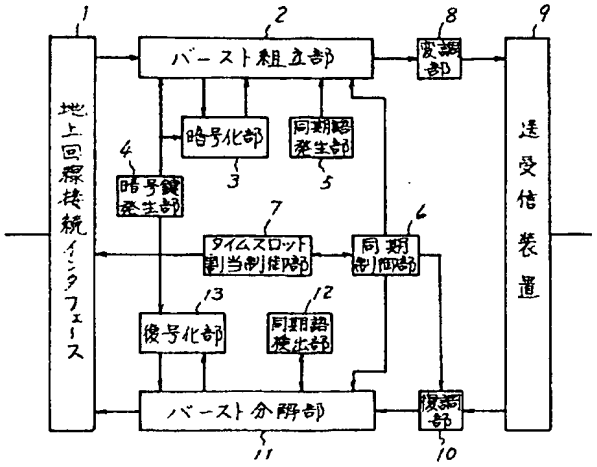
第 3 図



本第二の発明のデータバーストを例示する図

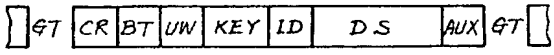
第 4 図

特開昭61-260735 (5)



従来例を示す図

第 5 図



従来あるデータバーストを例示する図

第 6 図

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.